



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/783,122

02/19/2004

Michael B. Shelby

IGT1P306X1/AC022 CIP

1230

79646

7590

07/21/2008

Weaver Austin Villeneuve & Sampson LLP - IGT

Attn: IGT

P.O. Box 70250

Oakland, CA 94612-0250

EXAMINER

DUFFY, DAVID W

ART UNIT

PAPER NUMBER

3714

MAIL DATE

DELIVERY MODE

07/21/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/783,122	<b>Applicant(s)</b> SHELBY ET AL.	
	<b>Examiner</b> DAVID W. DUFFY	<b>Art Unit</b> 3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 11 July 2008.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                       | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>05/27/2008</u>  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Status of Claims***

1. This office action is in response to the amendment filed 05/27/2008 in which applicant amends claims 1, 9, 16, 21, and 23. Claims 1-23 are pending.

### ***Continued Examination Under 37 CFR 1.114***

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/27/2008 has been entered.

### ***Priority***

3. Acknowledgment is made of applicant's revocation of claim for priority to Application No. 10/256,949, filed on 09/27/2002.

### ***Information Disclosure Statement***

4. The information disclosure statement (IDS) submitted on 05/27/2008 was filed after the mailing date of the Final Office Action on 12/26/2007. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

### ***Claim Rejections - 35 USC § 112***

5. Claims 1-8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which

was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 1 recites the limitation "generating a command originating at a master or slave server based upon an event at a gaming machine". The specification page 15, lines 12-13 which appears to be the basis for the limitation does not disclose the event occurring on a gaming machine, rather it describes a bonus event or winning occurring as the trigger. The description of the bonus system in the specification page 5, line 26 - page 6, line 2 describes the bonus event as occurring due to the accumulation of pool contributions reaching a predetermined level and a random determination by the master server matching a predetermined value in the master server. It is unclear how the trigger event may be based on an event at a gaming machine. Claims 2-8 depend from claim 1 and inherit the deficiency.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 16-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claim 16 recites the limitation "the digital signal" in the second to last line of the claim. There is insufficient antecedent basis for this limitation in the claim. For the purposes of examination it is assumed that 'the digital signature' was intended. Claims 17-20 inherit this deficiency.

***Claim Rejections - 35 USC § 103***

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-4, 8, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen, Binh T. US 20020071557 A1 in view of Federal Information Processing Standards Publication 186 (FIPS).

11. In regards to claim 1, Nguyen discloses generating a command based on an event at a gaming machine, digitally signing it and transmitting to a receiving node for re-hashing and verification (fig 4, elements 400-420). Nguyen does not explicitly disclose digitally signing the command by performing a hashing function over at least a portion of a message that includes the command to produce a message digest and passing the message digest through a digital signature algorithm to produce a digitally signed command; verification wherein the digitally signed command from the transmitting mode is subjected to the hashing function to produce a message digest, the message digest is passed through the digital signature algorithm to produce a digitally signed command at the receiving node, and the digitally signed command at the receiving node is compared to the digitally signed command from the transmitting mode to determine if there is a match.

12. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is

sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

13. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Nguyen in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks explicitly stating executing the command message at the subservient device, if the signatures verify.

14. However, as the goal of the system is to provide a secure communication system, it would be obvious to execute commands only if authorized and verified as otherwise the security of the system would be compromised. As such it would have been an obvious modification to make to have the device only execute commands that are verified and authorized

15. In regards to claim 2, Nguyen discloses that the gaming machine generates encrypted data messages based on machine transactions (fig 4, elements 400-406). Examiner contends that this constitutes monitoring events to generate a command.

16. In regards to claim 3, Nguyen discloses that the remote server or master of the system receives messages from the gaming machine and responds to the message (fig 4, elements 426-431). Examiner contends that this constitutes monitoring events on the

gaming machine by the master server as it receives event information from the gaming machine thereby monitoring the event. Nguyen further discloses that the local server or slave receives the signed command (fig 4, element 408).

17. In regards to claim 4, Nguyen discloses that the slave server processes and stores data generated by the gaming machine before re-encrypting and sending it to the master server (fig 4, element 412). Examiner contends that by storing the data the slave server is inherently monitoring the activities of the gaming machine. Nguyen further discloses sending a command from the master server to the gaming machine that the gaming machine verifies (fig 6).

18. In regards to claim 8, Nguyen discloses that encryption may be optional over a dedicated communication network and then applied when the message reaches an unsecured channel (11:39-47)

19. In regards to claims 16 and 17, Nguyen discloses the receiving of commands with digital signatures and verifying the signatures at a slave device (par 58). Nguyen lacks explicitly stating verifying the digital signature at the subservient device by subjecting the command message to a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a digital signature at the subservient device, and comparing the digital signature at the subservient device to the digital signature included with the command message to determine if there is a match; and executing the command message at the subservient device, if the signatures verify.

20. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

21. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Nguyen in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks explicitly stating executing the command message at the subservient device, if the signatures verify.

22. However, as the goal of the system is to provide a secure communication system, it would be extraordinarily obvious to execute commands only if authorized and verified as otherwise the security of the system would be compromised. As such it would have been an obvious modification to make to have the device only execute commands that are verified and authorized

23. In regards to claim 18, Nguyen discloses that the gaming device may receive signed messages and validate them (par 73).



24. In regards to claim 19, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62).

25. Claims 5-7 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen, Binh T. (US 20020071557 A1) in view of Federal Information Processing Standards Publication 186 (FIPS) as applied to claims 1 and 16 above, and further in view of Torango et al. (USPN 5885158).

26. In regards to claims 5 and 6, Nguyen in view of FIPS discloses the method of claim 1 above, but lacks wherein the event further comprises an event triggering a bonus is to be paid or wherein the command further comprises a bonus command.

27. In related prior art, Torango discloses a bonus system that generates bonus commands based on bonus triggering events (15:41-51). One skilled in the art would recognize the advantages of providing a progressive bonus game on a networked system in order to attract more players to a casino through higher potential payouts.

28. Therefore it would have been obvious to one skilled in the art at the time to combine the secure system of Nguyen in view of FIPS with the progressive system of Torango to provide a secure progressive system that would attract customers by offering larger potential payouts via a large group of networked devices.

29. In regards to claim 7, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62). Nguyen lacks explicitly stating that the message is a bonus command.

30. In related prior art, Torango discloses a bonus system that generates bonus commands (15:41-51). One skilled in the art would recognize the advantages of providing progressive games on a networked system to increase the size of the contributing player pool thereby offering larger potential payouts in order to attract players.

31. Therefore it would have been obvious to one skilled in the art at the time to combine the secure system of Nguyen with the progressive system of Torango to provide a secure progressive system thus providing large potential payouts to attract customers.

32. Nguyen in view of Torango lacks explicitly stating that the reply message is re-signed before sending it to the gaming machine.

33. However, Nguyen already discloses signing the messages on the way to the slave server from the gaming device (fig 4) and discloses that the slave server decrypts and then forwards the message to the gaming machine as stated above. It would be obvious to also re-encrypt and sign the message before sending it to the gaming machine as suggested by Nguyen.

34. In regards to claim 20, Nguyen in view of FIPS discloses the method of claim 16, but lacks disclosing the command comprising paying a bonus to a player at an electronic gaming machine.

35. In related prior art, Torango discloses a bonus system that generates bonus commands including paying a bonus (15:41-51). One skilled in the art would recognize the advantages of providing progressive games on a networked system to increase the

Art Unit: 3714

size of the contributing player pool thereby offering larger potential payouts in order to attract players.

36. Therefore it would have been obvious to one skilled in the art at the time to combine the secure system of Nguyen with the progressive system of Torango to provide a secure progressive system thus providing large potential payouts to attract customers.

37. Claims 9-15 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Torango et al. (USPN 5885158) in view of Nguyen, Binh T. (US 20020071557 A1) and Federal Information Processing Standards Publication 186 (FIPS).

38. In regards to claim 9, Torango discloses a progressive bonus system where the central server generates bonus commands (15:41-51). Torango further discloses the use of verification of hardware identification (16:1-13). Torango lacks disclosing performing a hashing function over at least a portion of a message that includes the bonus command to produce a message digest and then passing the message digest through a digital signature algorithm to produce a digitally signed bonus command; and transmitting the digitally signed bonus command from a transmitting node to an electronic gaming machine wherein the digitally signed bonus command from the transmitting mode is subjected to the hashing function to produce a message digest, the message digest is passed through the digital signature algorithm to produce a digitally signed bonus command at the gaming machine, and the digitally signed bonus

command at the gaming machine is compared to the digitally signed bonus command from the transmitting mode to determine if they match.

39. In related prior art, Nguyen discloses a system that is used to replace dedicated casino networks with secure communications over a general use network (par 15) where commands are digitally signed and transmitted to a gaming machine (par 62). Nguyen further discloses that some of the dedicated casino networks that may be replaced include network services for bonus game play, progressive game play and cashless ticketing (par 9). One skilled in the art would recognize the advantages of providing network security features to a networked progressive game system.

40. Therefore it would have been obvious to one skilled in the art at the time to combine the security system of Nguyen with the bonus system of Torango in order to provide a secure bonus system. The combination made lacks performing a hashing function over at least a portion of a message that includes the bonus command to produce a message digest and then passing the message digest through a digital signature algorithm to produce a digitally signed bonus command; and transmitting the digitally signed bonus command from a transmitting node to an electronic gaming machine wherein the digitally signed bonus command from the transmitting mode is subjected to the hashing function to produce a message digest, the message digest is passed through the digital signature algorithm to produce a digitally signed bonus command at the gaming machine, and the digitally signed bonus command at the gaming machine is compared to the digitally signed bonus command from the transmitting mode to determine if they match.

41. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

42. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Torango in view of Nguyen further in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process. The combination made lacks explicitly stating executing the command message at the subservient device, if the signatures verify.

43. However, as the goal of the system is to provide a secure communication system, it would be extraordinarily obvious to execute commands only if authorized and verified as otherwise the security of the system would be compromised. As such it would have been an obvious modification to make to have the device only execute commands that are verified and authorized

44. In regards to claim 10, Torango discloses monitoring gaming machine play (5:32-44).

Art Unit: 3714

45. In regards to claim 11, Torango discloses determining if a machine is to receive a bonus (15:41-51).

46. In regards to claims 12, Torango discloses the central server generating a bonus command (13:56-14:11).

47. In regards to claim 13, Torango discloses that the slave server monitors communication and provide verification of prize wins (16:1-23). Torango lacks explicitly disclosing that the slave server generates the bonus command. However, it is well known in the art of network systems to have mirrored servers doing the same tasks to compensate for any network outages or problems. As such, it would have been an obvious modification to provide the slave server with the ability to handle bonus commands on its own in the event that the central server was unreachable.

48. In regards to claim 14, Torango discloses that the bonus commands are sent to the game machine through the cluster controller (15-52-59). Torango lacks explicitly stating that the messages are signed.

49. In related prior art, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62). One skilled in the art would recognize the advantages of providing secure messages for a financial transaction system on an unsecured network.

50. Therefore it would have been obvious to one skilled in the art at the time to combine the bonus system of Nguyen with the security system of Torango in order to

provide a secure bonus server. The combination made lacks transmitting a second digitally signed bonus command to the electronic gaming machine.

51. However, Nguyen already discloses signing the messages on the way to the slave server from the gaming device (fig 4) and discloses that the slave server decrypts and then forwards the message to the gaming machine as stated above. It would be an obvious modification to also sign the message before sending it to the gaming machine as suggested by Nguyen as it would be mere duplication of steps.

52. In regards to claim 15, Torango in view of Nguyen and FIPS disclose the method of claim 9 above, but lacks wherein the method comprises transmitting an unsigned message after the generation of the bonus command and digitally signing the bonus command at a slave server. Rather the combination teaches signing the messages at the master server.

53. However, it would have been obvious to one skilled in the art that the operator of the game system would have the choice to use security measures on whatever portions of the system they chose as such a matter would have been mere design choice that fails to distinguish over the prior art.

54. In regards to claim 21, Torango discloses a bonus server system that pays bonuses to players as directed (15:41-51) and further discloses that the gaming machines are verified by machine signatures and if invalid, the bonus is canceled (16:4-15). Torango lacks a digital signature; verifying the digital signature at a subservient device by subjecting the bonus message to a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a

digital signature at the subservient device, and comparing the digital signature at the subservient device to the digital signal included with the command message to determine if there is a match.

55. In related prior art, Nguyen discloses a system that is used to replace dedicated casino networks with secure communications over a general use network (par 15) where commands are digitally signed and transmitted to a gaming machine (par 62). Nguyen further discloses that some of the dedicated casino networks that may be replaced include network services for bonus game play, progressive game play and cashless ticketing (par 9). One skilled in the art would recognize the advantages of providing network security features to a networked progressive game system.

56. Therefore it would have been obvious to one skilled in the art at the time to combine the security system of Nguyen with the bonus system of Torango in order to provide a secure bonus system. The combination made lacks subjecting the bonus message to a hashing function to produce a message digest, passing the message digest through a digital signature algorithm to produce a digital signature at the subservient device, and comparing the digital signature at the subservient device to the digital signal included with the command message to determine if there is a match.

57. In related prior art, FIPS discloses a digital signature standard that digitally signs a message by using a hash function in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The



verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. One skilled in the art would recognize the advantages of providing a secure way to authenticate the sender of a message in a network environment.

58. Therefore it would have been obvious to one skilled in the art at the time of the invention to have modified Torango in view of Nguyen further in view of FIPS in order to have included the digital signature method of FIPS in order to provide a secure authentication process.

59. In regards to claim 22, Torango discloses manual intervention to resolve invalid payouts (16:15-21).

60. In regards to claim 23, Torango discloses that the bonus commands are sent to the game machine through the cluster controller (15-52-59). Torango lacks disclosing verifying the digital signature at the subservient device comprising generating a second command message, providing a digital signature to the second command message and transmitting the second command message with the digital signature.

61. In related prior art, Nguyen discloses generating a signed command at the master server, sending it to the slave server, and the slave server decrypting the message and forwarding to the gaming machine (par 62). One skilled in the art would recognize the advantages of providing secure messages for a financial transaction system on an unsecured network.

62. Therefore it would have been obvious to one skilled in the art at the time to combine the bonus system of Torango with the security system of Nguyen in order to provide a secure bonus server. The combination made lacks explicitly stating that the reply message is re-signed before sending it to the gaming machine.

63. However, Nguyen already discloses signing the messages on the way to the slave server from the gaming device (fig 4) and discloses that the slave server decrypts and then forwards the message to the gaming machine as stated above. It would be obvious to also re-encrypt and sign the message before sending it to the gaming machine as suggested by Nguyen.

#### ***Response to Arguments***

64. Applicant's arguments filed 05/27/2008 have been fully considered but they are not persuasive. Applicant argues that Nguyen does not disclose command originating at a master server. Examiner respectfully disagrees. Nguyen discloses sending a response message to a game machine upon receipt of a message. The message sent by the central server is not the same message sent by the gaming machine. The new message originates at the server.

65. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

66. Nguyen teaches a secured network system to ensure that data sent through the system is protected from malicious outsiders. FIPS teaches a method of determining the sender of a digital message to ensure the veracity of the message and its sender. One skilled in the art would recognize the advantages of the combination of these system to provide a secured network with secured messages that provide verifiable notification of the sender and the contents of the message. It would be extraordinarily obvious to only execute commands that were verified and from authorized senders as otherwise the entire security of the system would be purely for show.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID W. DUFFY whose telephone number is (571)272-1574. The examiner can normally be reached on M-F 0830-1700.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Xuan M. Thai can be reached on (571) 272-7147. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 3714

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. W. D./  
Examiner, Art Unit 3714

/Corbett Coburn/  
Primary Examiner  
AU 3714